DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

June 2020

(Sent on behalf of your ISR)

Dear FSO,

This monthly newsletter contains recent information, policy guidance, security education, and training updates. If you have any questions or recommendations for information to be included, please feel free to let us know.

WHERE TO FIND BACK ISSUES OF THE VOICE OF INDUSTRY (VOI) NEWSLETTER

Missing a few back issues of the VOI Newsletter? The VOI Newsletters, important forms, and guides may be found on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools Page (VOIs are at the bottom of the page). For more information on personnel vetting, industrial security, or any of the other topics in the VOI, visit our website at www.dcsa.mil.

TABLE OF CONTENTS

INDUSTRIAL SECURITY OPERATIONS

JAMES S. COGSWELL INDUSTRIAL SECURITY AWARD PROGRAM

As a result of the COVID-19 pandemic and the cancellation of the National Classification Management Society (NCMS) 56th Annual Training Seminar in June, DCSA will publicly announce the 2020 James S. Cogswell Industrial Security Award winners on July 30 in lieu of conducting a ceremony. DCSA's Office of Communications and Congressional Affairs will release the 2020 award winner's information via press release, Twitter, Facebook, as well as through other media outlets. Additionally, we will publish the award winners by company name in the July VOI Newsletter.

After the announcement is made, the awards will be mailed directly to the recipients, and a DCSA representative will present the awards to the leadership of each winning facility at a mutually convenient time, either in person (when travel is deemed safe), or virtually.

We look forward to announcement of the well deserving winners for 2020, despite the current health and safety conditions.

OVERNIGHT EXPRESS DELIVERY UPDATE (FEDEX AND UPS)

The Information Security Oversight Office (ISOO) has advised OUSD(I&S) and DCSA that GSA has confirmed that FedEx and UPS continue to serve as authorized carriers for overnight express delivery that meets the requirements of National Industrial Security Program Operating Manual (NISPOM) 5-403.e and guidance outlined in Industrial Security Letter (ISL) 2014-01. The current agreements with GSA for FedEx and UPS continues through September 30, 2022. ISOO, OUSD(I&S), DCSA, USTRANSCOM, and GSA will be meeting to address continued guidance and issues related to access to information that allows contractors to verify approved carriers for overnight express delivery. DCSA will keep Cleared Industry updated on any changes and updates to the program.

NISP AUTHORIZATION OFFICE (NAO)

ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE VERSION 5.7.2

The Defense Information Systems Agency recently released the Enterprise Mission Assurance Support Service (eMASS) Version 5.7.2. The update includes improvements to streamline Risk Management Framework assessment and authorization activities. The new features include:

1. Additional system-level fields on the System Details page (Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and Protected Health Information (PHI))
2. Sub-section for System Location on the System Details page
3. Updated filters on the Controls Listing page for identifying incomplete Assessment Procedures (AP) and Non-Compliant (NC) APs that lack a Plan of Action and Milestone (POA&M) item, and
4. Added filtering options for the Executive Level Dashboard Reports.

For additional information, visit the [Help] page in eMASS. Refer questions or concerns through the NAO eMASS Mailbox.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

NISS 2.2.1 UPGRADE

We continue to make updates in NISS to improve the customer service experience and develop new functionality for our users. The NISS team successfully deployed the 2.2.1 upgrade on June 15. The information is posted as an article in the in-system Knowledge Base entitled "System Updates: Release 2.2.1."

UPDATE ON INDUSTRIAL FACILITY PROFILE UPDATES FEATURE

The Full Operational Capability (FOC) for Industrial Facility Profile Updates was released as part of the NISS 2.2.1 upgrade. FOC gives Industry the ability to suggest updates to information on the Safeguarding & IS tab. The job aid for Industrial Facility Profile Updates can be found in the Knowledge Base under "Facility Profile Update Request - Full Operational Capability."

Your feedback is very important to us. Please submit requests for new functionality or for enhancements to existing functionality to DCSA.NISSRequirements@mail.mil.

For technical issues with NCAISS or NISS, continue to contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance and Option 2 again for NISS.

VETTING RISK OPERATIONS CENTER (VROC)

INDUSTRY FINGERPRINT SUBMISSIONS FOR BACKGROUND INVESTIGATIONS

The Under Secretary of Defense for Intelligence and Security provided personnel vetting guidance for the continued collection and processing of fingerprints. The guidance states that DoD, to the greatest extent possible, will continue to follow established guidance for vetting contractors under DoD cognizance for the NISP.

Please refer to list of fingerprint service providers supporting geographic areas across the country at the DMDC Personnel Security Assurance website.

For investigation requests where the fingerprint check is completed, please submit the investigation request to VROC. The fingerprint check will result in a SAC investigation populated on the Joint Personnel Adjudication System (JPAS) Person Summary Screen. The SAC investigation is valid for 120 days from the closing date.

If the fingerprint check was not completed, it is requested that the investigation request not be submitted to VROC until the fingerprints are captured and submitted to SWFT for processing. For investigation requests that have been submitted to VROC without fingerprint submissions, VROC will hold the investigation request until the SAC is populated in JPAS.

VROC will continue to monitor the impacts of COVID 19 and the investigation submission process. If you have any questions, please contact the VROC Knowledge Center.

RRU TO CSR TRANSITION

On June 1, the Defense Manpower Data Center (DMDC) disabled the Research, Recertify and Update (RRU) functionalities in JPAS. All Customer Service Requests (CSRs) to include RRU requests and Non-Disclosure Agreements (NDAs) (SF312s) must now be submitted via the Defense Information System for Security (DISS) application. For instructions on how to complete CSR/NDA actions, please reference the user manual under the Help link on the DISS Joint Verification System (JVS) application or review the VROC DISS Tips and Tricks here. To avoid any disruption of service, it is imperative to obtain a DISS account to ensure a seamless transition from JPAS to DISS. For additional questions or concerns, please contact the VROC Knowledge Center.

DISS AUTO-PROVISIONING

DMDC is conducting automated provisioning of DISS JVS accounts for the Industry Security Management Offices. This is one of the major steps in fully deploying DISS within the DoD as the JPAS replacement. Eligible recipients will receive two email notifications: one with user provisioning instructions, and the second with credentials to access the DISS JVS application. For those who wish to manually request a DISS account, please follow the PSSAR Industry instructions on the DMDC website or email the Industry Provisioning Team.

E-QIP RESET INQUIRIES CHANGE

VROC appreciates your patience as we have attempted to find the appropriate means to provide Industry e-QIP reset customer support during the COVID 19 pandemic. Effective April 20, ONLY Industry e-QIP resets will be handled by the DCSA Applicant Knowledge Center. Please call 724-738-5090 or email DCSA Applicant Support for assistance. For ANY other Personnel Security Clearance Inquiries, please email the VROC Knowledge Center or submit a CSR via DISS.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

The DCSA NAESOC provides NISP oversight for assigned "Access Elsewhere" facilities. Its mission includes supporting optimal security oversight tailored to the specific requirements of non-possessor facilities.

The following reminders are provided for our customers. To keep abreast of the latest updates and NAESOC items of interest, please check the NAESOC web page.

Contacting the Help Desk: Customers may leave a detailed voicemail message at 1-888-282-7682, Option 7, to include your name, phone number, facility name and CAGE Code, and a brief summary of the reason for your call. All voicemails will be responded to within one business day. Alternatively, you may send a message using NISS Messenger or send an email to the NAESOC Mailbox.

Reporting Security Violations: Remember, in addition to reporting security violations taking place at your location and/or affecting your facility's assets, security violations that take place at Government locations, military installations, and/or other contractor sites are reportable to DCSA. Reports should be made via NISS Messenger.

Security Review Engagements: All Continuous Monitoring (CM) engagements and Virtual Security Reviews will be conducted telephonically. Please ensure contact information in your NISS profile for the Senior Management Official (SMO), Facility Security Officer (FSO), and Insider Threat Program Senior Official (ITPSO) are current. In addition, remember that we are not issuing ratings at this time for our CM engagements.

Facility Profile Updates: Since NISS now has the capability to allow you to "Request Facility Profile Updates" and make changes to your company's NISS profile, all FSOs should routinely review their NISS profiles and make any necessary updates. The NAESOC will no longer be asking for Request for Information prior to CM engagements, but will expect the facility to complete any profile updates as they happen. We will validate the information during security review engagements.

Facility Clearance (FCL) Packages (Change Conditions): Please ensure your FCL Package submissions include the supporting business documents for the changes you are reporting. Our goal is to provide rapid response and service for you. Your help in ensuring the documentation is submitted expedites that effort.

Oversight Requirement Reminder for Branch/Division Offices Transferred to NAESOC: Per ISL 2006-02 #7, non-possessing divisions do not require an FCL except under rare circumstances. Any non-possessing branch/division office identified by NAESOC will receive a letter of intent to Administratively Terminate the FCL unless justification is received by NAESOC within 30 days. The NAESOC is committed to working with companies under its purview on the requirement for maintaining their FCLs. For additional questions or concerns, please see our contact information below.

Speaking Events: We are actively participating in Industry information sharing events and accepting invitations to virtual meetings. Please send an email to the NAESOC Mailbox and we will be happy to work out the details.

Use NISS for:

- FCL Package – Report all Changed Conditions
- DD Form 441s (FEB 2020) – Now updated to accept electronic signatures
- Messenger Box – Report all Security Violations
- Facility Profile Update Requests – this allows you to provide real time updates; information that can be edited by Industry users includes, but is not limited to new contracts, program assets, and Key Management Personnel contact information.

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email the NAESOC Mailbox (Subject Line: Facility Name & CAGE Code)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

INSIDER THREAT SENTRY APP NOW AVAILABLE

The Insider Threat Sentry mobile app is finally here! Made with the vigilant user in mind, it allows you to download posters, play vigilance learning games, watch videos, and find the toolkit items you need to promote awareness all year long. Insider Threat Sentry is available in the app store for Android and iOS. Learn more about app features and what you can expect by watching this video.

JUNE PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In June, we released the sixth in a series of monthly security awareness newsletters called CDSE Pulse. The June newsletter featured Personnel Vetting content. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription and get the newsletter sent directly to your inbox by submitting your email address at CDSE News.

JULY COUNTERINTELLIGENCE (CI) SPEAKER SERIES

CDSE invites you to participate in our upcoming CI Speaker Series:

- 2019 Targeting U.S. Technologies Report
  Thursday, July 23, 2020
  12:00 – 1:00 p.m. ET

Please join this live event as DCSA and CDSE discuss the latest trends in foreign targeting of U.S. defense technologies. Register for all webinars at CDSE Webinars.

UPCOMING "KNOW YOUR CDSE" SPEAKER SERIES

As part of CDSE's 10th Anniversary, we launched a "Know Your CDSE" Speaker Series featuring a different security focus for each webinar. CDSE invites you to participate in our July and August Speaker Series that will feature our training, resources, and processes for CI Awareness, Special Access Programs (SAPs), and Certification.

- Know your CDSE: Counterintelligence
  Thursday, July 9, 2020
  12:00 p.m. - 12:30 p.m. ET
- Know your CDSE: Special Access Programs
  Thursday, July 30, 2020
  12:00 p.m. - 12:30 p.m. ET
- Know Your CDSE: Certification
  Thursday, August 13, 2020
  12:00 p.m. - 12:30 p.m. ET

Do not miss this opportunity to learn how to enhance your CI Awareness, understanding of SAPs, and expand your knowledge of our Certification Program. Register now for all three events!

NEWLY ARCHIVED SPEAKER SERIES

Did you miss any of our April Speaker Series? No problem! Access these archived topics:

- Counterintelligence, the Supply Chain, and You
- Know Your CDSE: Insider Threat

You will have the option of viewing the recording that includes either the training certificate or the one without the certificate. Check out all of our Speaker Series and webinars in the On Demand Webinars (includes CDSE Certificates of Training) and the Previously Recorded Webinars (does not include certificates).

NEWLY UPDATED JOB AID - RECEIVE AND MAINTAIN YOUR NATIONAL SECURITY ELIGIBILITY

CDSE's updated job aid breaks down the national security eligibility process, including position designation, adjudicative guidelines, due process, continuous evaluation, and self-reporting. The updated job aid replaces the "Receive and Maintain Your Security Clearance" job aid. View and download the Receive and Maintain Your National Security Eligibility job aid today!

NEW INSIDER THREAT CASE STUDY

CDSE recently released a new Insider Threat Case Study, Shamai Leibowitz. This case study can easily be included in an organization's security education, training, and awareness programs. CDSE case studies are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Find them here.

Access this new case study today!

NEW INSIDER THREAT TOOLKIT TAB – INTERNATIONAL MILITARY STUDENTS

CDSE added a new tab to its Insider Threat Toolkit, providing a centralized location for insider threat awareness resources to support International Military Students and insider threat practitioner resources for International Military Student Officers, Faculty, and Staff at US training locations. Explore the new International Military Students tab offerings here.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE